#4 04DD

Attorney Docket No. 1573.1010

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Koichi ITO, et al.

Application No.: 10/028,265 Group Art Unit:

Filed: December 28, 2001 Examiner:

For: ENCRYPTION SECURED AGAINST DPA

INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the duty of disclosure provisions of 37 CFR § 1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the subject application.

1. Enclosures accompanying this Information Disclosure Statement are:

   1a. ☒ Form PTO-1449.
   1b. ☒ Copies of IDS citations.
   1c. □ An English language copy of search report(s) from a counterpart foreign application or a PCT International Search Report.
   1d. □ English language translation (complete or relevant portion(s)) attached to each non-English language publication.
   1e. ☒ Explanations of Relevancy of References (ATTACHMENT 1(e), hereto) for providing a concise explanation of each non-English publication.
   1f. □ List of Copending Applications (ATTACHMENT 1(f), hereto).
   1g. □ List of Additional Submitted Documents (ATTACHMENT 1(g), hereto).

2. ☒ This Information Disclosure Statement is filed under 37 CFR §1.97(b):

   (Check either Item 2a or 2b or 2c or 2d)

   2a. □ Within three months of the filing date of a national application other than a Continued Prosecution Application under § 1.53(d);
   2b. □ Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application.
   2c. ☒ Before the mailing of a first Office Action on the merits; or
   2d. □ Before the mailing of a first Office Action after the filing of a Request for Continued Examination under § 1.114.

3. □ This Information Disclosure Statement is filed under 37 CFR § 1.97(c) after the period specified in paragraph 2 above but before the mailing date of any of a Final Office Action under § 1.113, a Notice of Allowance under § 1.311 or an action that otherwise closes prosecution in the application, AND

(*Check either Item 3a or 3b; Item 3b to be checked if any reference known for more than 3 months*)

3a. □ The §1.97(e) Statement in Item 5 below is applicable; OR
3b. □ The $180.00 fee set forth in 37 C.F.R. §1.17(p) is:
□ enclosed.
□ to be charged to Deposit Account No. 19-3935.

4. □ This Information Disclosure Statement is filed under 37 CFR §1.97(d) after the period specified in paragraph 3 above, but on or before payment of the Issue Fee, AND

4a. □ The § 1.97(e) Statement in Item 5 below is applicable; AND
4b. □ The $180.00 fee set forth in 37 C.F.R. §1.17(p) is:
□ enclosed.
□ to be charged to Deposit Account No. 19-3935.

5. □ Statement under § 1.97(e) (*applicable if Item 3a or Item 4 is checked*)

(*Check either Item 5a or 5b*)

5a. □ In accordance with 37 CFR § 1.97(e)(1), it is stated that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. □ In accordance with 37 CFR § 1.97(e)(2), it is stated that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known by any individual designated in §1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

6. □ This is a continuation/divisional/continuation-in-part application under 37 CFR § 1.53(b).

(*Check appropriate Items 6a and/or 6b*)

6a. □ Copies of the publications listed on the attached Form PTO-1449 which were previously cited in prior application Serial No. __, filed on __, and which is relied on for an earlier effective filing date for the subject application under 35 U.S.C. § 120, have been omitted pursuant to 37 CFR § 1.98(d).

6b. □ Copies of the publications listed on the attached Form PTO-1449 which were not previously cited in prior application Serial No. __, filed on __, and which is relied on for an earlier effective filing date for the subject application under 35 U.S.C. § 120, are provided herewith.

7. □ This is a continuation/divisional application under 37 CFR § 1.53(d) or Request for Continued Examination under 37 CFR 1.114.

(*Check either Item 7a or 7b*)

7a. □ The Issue Fee has not been paid.
7b. □ A Petition to Withdraw from issue under 37 CFR §1.313(c) is filed concurrently herewith or has been granted. A continuation application under 37 CFR § 1.53(d) or Request for Continued Examination under 37 CFR 1.114, after payment of the Issue Fee is proper in accordance with 37 CFR § 1.53(d)(1)(ii) or 37 CFR 1.114(a), respectively.

8. □ This is a Supplemental Information Disclosure Statement.

(*Check either Item 8a or 8b*)

8a. □ This Supplemental Information Disclosure Statement under 37 CFR § 1.97(f) supplements the Information Disclosure Statement filed on __. A bona fide attempt was made to comply with 37 CFR § 1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental IDS can be considered as if properly filed on __.
8b. □ This Supplemental Information Disclosure Statement is timely filed within one (1) month of the Notice under 37 CFR § 1.97 and 1.98, mailed __. (MPEP 609 C(1), Form ¶ 6.49, Rev. 1, Feb. 2000, pp. 600-107)

9. ☒ In accordance with 37 CFR § 1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(*Check appropriate Items 9a, 9b, 9c and/or 9d*)

9a. □ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office. (See U.S. Patent & Trademark Office's authorization in the Federal Register, Vol. 57, No. 12, January 17, 1992, at page 2031 (Reply to Comment 68).)
9b. □ set forth in the application.
9c. ☒ satisfied because an English language translation (complete or relevant portion(s)) is attached to each non-English language publication.
9d. ☒ enclosed as Attachment 1(e), hereto.

10. No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than search report(s) from a counterpart foreign application or a PCT International Search Report, if submitted herewith). 37 CFR §§ 1.97(g) and (h).

11. The Commissioner is authorized to credit any overpayment or charge any additional fee required under 37 CFR § 1.17 for this Information Disclosure Statement and/or Petition to Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

By: ______________________
H. J. Staas
Registration No. 22,010

Dated: February 1, 2002
700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

Sheet 1 of 2

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

LIST OF REFERENCES CITED BY APPLICANT

(Use several sheets if necessary)

ATTORNEY DOCKET NO. 1573.1010	APPLICATION NO. 10/028,265
FIRST NAMED INVENTOR Koichi ITO, et al.	
FILING DATE December 28, 2001	GROUP ART UNIT

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE
	AA						
	AB						
	AC						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION	
							YES	NO
	AD	2000-305453	11/2000	Japan			X	
	AE	WO 99/67919	12/1999	WIPO			X	
	AF	WO 00/46953	08/2000	WIPO			X	
	AG	WO 00/27068	05/2000	WIPO			X	
	AH	WO 00/49765	08/2000	WIPO			X	
	AI	WO 01/10077	02/2001	WIPO			X	

OTHER REFERENCES *(Including Author, Title, Date, Pertinent Pages, Etc.)*

	AJ	Kocker, Paul, et al., "Differential Power Analysis" in Proceedings of Advances in Cryptology-CRYPTO '99, Springer-Verlag 1999. pages 388-397.
	AK	Messerges, Thomas, et al., "Power Analysis Attacks of Modular Exponentiation in Smartcards", Cryptographic Hardware and Embedded Systems (CHES '99), Springer-Verlag, pages 144-157
	AL	Akkar, Mehdi-Laurent, et al., "Power Analysis, What is Now Possible...", ASIACRYPT 2000, Pages 489-502.
	AM	Messerges, Thomas S., "Securing the AES Finalists Against Power Analysis Attacks", Proceedings of Fast Software Encryption Workshop 2000, Springer-Verlag, April 2000, which is called "a masking method."

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Sheet 2 of 2

FORM PTO-1449	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NO. 1573.1010	APPLICATION NO. 10/028,265
LIST OF REFERENCES CITED BY APPLICANT		FIRST NAMED INVENTOR Koichi ITO, et al.	
(Use several sheets if necessary)		FILING DATE December 28, 2001	GROUP ART UNIT

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE
	BA						
	BB						
	BC						
	BD						
	BE						
	BF						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	NO
	BG	WO 00/24155	04/2000	WIPO			X	
	BH	WO 00/24156	04/2000	WIPO			X	
	BI							
	BJ							
	BK							
	BL							

OTHER REFERENCES *(Including Author, Title, Date, Pertinent Pages, Etc.)*

	BM	Messerges, Thomas S. et al., "Investigations of Power Analysis Attacks on Smartcards", Proceedings of USENIX Workshop on Smartcard Technology, March 1999.
	BN	Chari, Suresh, et al., "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", Second Advanced Encryption Standard Candidate Conference, March 1999.
	BO	FIPS 46, "Data Encryption Standard" Federal Information Processing Standards Publication 46, U.S. Departement of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, VA, 1977.
	BP	http://csrc.nist.gove/encryption/aes/rijndael/Rijndael.pdf (which is linked from http://www.nist.gov/aes/).

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609: Draw line through citation if

ATTACHMENT 1(e)

EXPLANATIONS OF RELEVANCY OF REFERENCES

ATTORNEY DOCKET NO. 1573.1010	APPLICATION NO. 10/028,265
FIRST NAMED INVENTOR Koichi ITO, et al.	
FILING DATE December 28, 2001	GROUP ART UNIT

Reference AD is one type of random masking method, which has lower security than the original.

Reference AE is doubling plaintext messages and secret keys, randomizing bit permutation, and updating plaintext/secret key data in each round.

Reference AF is multiplexing data.

Reference AG is one type of random masking method.

Reference AH is one type of random masking method.

Reference AI is a random masking method specialized for DES structure.

Reference AJ is a power analysis (DPA and SPA) of DES implementations.

Reference AK is DPA of RSA implementations.

Reference AL is DPA in power consumption models.

Reference AM is Messerges' random masking method.

References BG and BH are methods for employing combination of transform tables S[x], ~S[x], S[~x] and ~S[~x], where S[x] represents an Sbox transform table for conventional DES and "~a" represents inverted {a} having 0's and 1's.

Reference BM is an experiment showing power dissipation depending on the number of "0" or "1" bits in loaded data.

Reference BN is DPA of Rijndael implementations.

Reference BO is the specification of DES.

Reference BP is the specification of Rijndael Cipher.